Diana Carolina Donoso Casas

 ddonosoc@cajaviviendapopular.gov.co

Oficina de Tecnologías de la Información y las Comunicaciones

Bogotá D.C., Julio de 2018
Versión 1.0

PLAN DE TRATAMIENTO DE RIESGOS dE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAJA DE LA VIVIENDA POPULAR

**TABLA DE CONTENIDO**

[1. OBJETIVO 2](#_Toc520717009)

[2. ALCANCE 2](#_Toc520717010)

[3. RESPONSABLES 2](#_Toc520717011)

[4. DEFINICIONES 2](#_Toc520717012)

[5. DOCUMENTOS DE REFERENCIA 4](#_Toc520717013)

[6. METODOLOGÍA 5](#_Toc520717014)

[6.1. Criterios de Frecuencia 5](#_Toc520717015)

[6.2. Criterios De Impacto 6](#_Toc520717016)

[6.3. Mapa de Calor de Riesgos 6](#_Toc520717017)

[6.4. Tratamiento del Riesgo 8](#_Toc520717018)

[7. PLAN DE TRATAMIENTO DE RIESGOS 9](#_Toc520717019)

[8. CONTROL DE CAMBIOS 13](#_Toc520717020)

# **OBJETIVO**

Establecer los lineamientos de buenas prácticas de seguridad y privacidad de la información, que permita definir criterios para la identificación, análisis, valoración y gestión de los riesgos potenciales que afecten la confiabilidad, disponibilidad e integridad de la información de la Caja de la Vivienda Popular.

# **ALCANCE**

El presente Plan de Tratamiento aplica para toda la Caja de la Vivienda Popular, funcionarios, contratistas y terceros, que tengan acceso, usen, produzcan o manejen información de los procesos estratégicos, misionales, de apoyo y de evaluación, de la Entidad.

# **RESPONSABLES**

El Responsable por la actualización del Manual es la Oficina de Tecnología de Información y las Comunicaciones – TIC.

# **DEFINICIONES**

A continuación, se relacionan los conceptos y definiciones aplicables al presente plan:

* ***Activos de Información***: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
* ***Amenazas***: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
* ***Análisis de Riesgo***: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
* ***Confidencialidad***: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
* ***Control***: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
* ***Disponibilidad***: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
* ***Encargado del Tratamiento de Datos***: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
* ***Gestión de incidentes de seguridad de la información***: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000
* ***Información***: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
* ***Información Clasificada***: Es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a ciertos derechos, contemplados en la misma ley.
* ***Información Reservada***: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
* ***Integridad***: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
* ***No repudio***: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
* ***Plan de continuidad del negocio***: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
* ***Plan de tratamiento de riesgos***: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
* ***Privacidad***: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
* ***Riesgo***: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
* ***Sistema de Gestión de Seguridad de la Información SGSI***: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000)
* ***Seguridad de la Información***: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad.
* ***Tecnología de la Información***: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

# **DOCUMENTOS DE REFERENCIA**

La Caja de la Vivienda Popular ha elaborado el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, tomando como referencia Norma NTC-ISO-IEC 27001, que es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

Adicionalmente, tiene en cuenta lo establecido en el Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

En particular la Guía No. 7, MINTIC, Guía de gestión de riesgos, Seguridad y privacidad de la información.

# **METODOLOGÍA**

La Caja de la Vivienda Popular cuenta con el Procedimiento de Administración del Riesgo, el cual se encuentra dentro del Proceso Gestión Estratégica, el cual establece un esquema adaptado e integrado a los procesos de la entidad que aporte al logro de los objetivos y facilite la mejora continua, mediante el análisis de la incertidumbre como un factor que se puede manejar a través del uso de información y conocimiento para la toma de decisiones acertadas frente a posibles eventos y sus efectos adversos.

Dentro de esta metodología para la valoración de los riesgos se tienen en cuenta los siguientes criterios:

# **Criterios de Frecuencia**

***Excepcional***: Puede ocurrir sólo en circunstancias excepcionales y bajo condiciones muy puntuales.

***Improbable***: Puede ocurrir en algún momento, pero su probabilidad de ocurrencia es casi nula.

***Posible***: Puede ocurrir en algún momento bajo circunstancias normales

***Probable***: La probabilidad de que ocurra bajo condiciones normales alta

***Casi Seguro***: Se espera que ocurra en la mayoría de las circunstancias

# **Criterios De Impacto**

***Insignificante***: El riesgo no conlleva a consecuencias significativas, la afectación es insignificante en temas referentes al cumplimiento de objetivos.

***Menor***: El riesgo conlleva a consecuencias mínimas, la afectación en temas referentes al cumplimiento de objetivos presenta niveles bajos.

***Moderado***: La materialización de este riesgo conllevaría a consecuencias y afectaciones moderadas, de no darse un manejo adecuado, puede verse comprometido el cumplimiento de objetivos de los procesos.

***Mayor***: La materialización de este riesgo conlleva a afectaciones mayores, contempla tratamiento médico en vidas humanas y compromete el cumplimiento de los objetivos de los diferentes procesos.

***Catastrófico***: El Riesgo afecta negativamente la vida y/o bienes inmuebles y representa una enorme pérdida financiera. Si el riesgo es de un proceso de apoyo, estratégico o de evaluación, su materialización impide el cumplimiento del objetivo del proceso.

# **Mapa de Calor de Riesgos**

Una vez determinado el nivel de frecuencia y consecuencia del riesgo se debe estimar el nivel de riesgo a través de la ubicación en la siguiente matriz de Nivel de Riesgo. Así se determinará el nivel de riesgo al que está expuesto el proceso por la materialización de los factores identificados previamente.



De acuerdo con los resultados obtenidos en la valoración de riesgos podemos obtener los siguientes resultados:

***Extremo***: Zona de nivel de riesgo en la que es aconsejable eliminar el factor que genera el riesgo en la medida que sea posible. Se deben implementar acciones de prevención para tratar de eliminar la frecuencia del riesgo y/o disminuir el Impacto mediante acciones de mitigación.

***Alto***: Zona de nivel de riesgo en que las consecuencias deben ser controladas con acciones. En este nivel de riesgo se deben tomar Acciones y controles que lleven en lo posible al riesgo a zonas moderada y baja.

***Medio***: Zona de nivel de riesgo en que posible asumirlo, es decir, el riesgo se encuentra en un nivel que puede ser aceptado tras la implantación de algunas medidas de control diferentes a las que se poseen.

***Bajo***: Estos riesgos son los de menor frecuencia de ocurrencia y más bajo impacto, sin embargo, representan una posible alteración al normal desarrollo de las labores de la entidad, por lo tanto, pueden asumirse.

# **Tratamiento del Riesgo**

Para dar desarrollo de este importante componente de la administración de riesgos, es prioritario resaltar que en la definición de las metas se contemple la fácil medición y por ende la realización de estas en un periodo de tiempo determinado. De esta manera se debe fijar una meta obligatoria para cada riesgo identificado y clasificado en la zona de riesgo como Altos o Extremos, teniendo en cuenta los siguientes aspectos:

* El límite de tiempo para la ejecución de la acción será de un año a partir de la aprobación del Mapa de Riesgos.
* Tener en cuenta aspectos de viabilidad jurídica, técnica, institucional y financiera.

***Criterios para el tratamiento del riesgo***

***Mitigar***: Se desarrolla mediante la generación de cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

***Prevenir***: La prevención del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

***Dispersar***: Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

***Transferir***: Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros, esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

***Asumir***: Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

# **PLAN DE TRATAMIENTO DE RIESGOS**

Siguiendo la metodología de Administración de Riesgos con que cuenta la Entidad, se ha desarrollado la evaluación de Riesgos al Proceso Gestión de Tecnologías de la Información y las Comunicaciones.

En primera instancia se elabora la matriz DOFA, en donde se identifican los factores tanto positivos como negativos que afectan al proceso. El resultado se puede apreciar en la siguiente gráfica:



Posteriormente se identifican tres riesgos principales relacionados con los procedimientos que componen el proceso evaluado. A continuación, se muestra la información general de los riesgos identificados, la información detallada se puede encontrar en el documento “***Matriz de Riesgos TIC.xlsx***”.

***Riesgo 1:***



***Tratamiento***:



***Riesgo 2***:



***Tratamiento***:



***Riesgo 3***:



***Tratamiento***:



# **CONTROL DE CAMBIOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha Aprobación (dd-mm-aaaa)** | **Cambios** | **Revisó (Nombre y Cargo)** |
| 1 | 27-07-2018 | Creación del documento | Diana Carolina Donoso CasasJefe Oficina TIC  |